Amendments to the claims,
Listing of all claims pursuant to 37 CFR 1.121(c)

This listing of claims will replace all prior versions, and listings, of claims in the application:

What is claimed is:

1. (Currently amended) A method for controlling connections to a new computer upon its initial deployment, the method comprising:

before deployment of the new computer, imaging the computer's storage to include a preconfigured security update policy for preventing Internet-borne infections occurring before the computer can obtain security-relevant updates;

upon the initial deployment of the new computer, applying ~~a~~ said preconfigured security update policy to establish at the computer ~~that establishes~~ a pre-access restricted zone of at least one preapproved host that the computer ~~may~~ is restricted to connect to upon its initial deployment for obtaining current security-relevant updates, so that the computer is ~~not allowed to participate with general~~ completely blocked from all other connectivity to the Internet until security-relevant updates have been completed;

receiving a request for a connection from the computer to a particular host;

based on said preconfigured security update policy, determining whether the particular host is within the restricted zone of at least one preapproved host;

blocking said connection if said particular host is not within the restricted zone of at least one preapproved host; and

once the computer has complied with the security update policy, lifting the restricted zone so that the computer is allowed to participate with general connectivity to the Internet.

2. (Previously presented) The method of claim 1, further comprising:

prior to the initial deployment of the computer, imaging a hard disk of the computer with said preconfigured security update policy.

3. (Previously presented) The method of claim 1, wherein the computer comprises a portable computer and the initial deployment includes establishing Internet

connectivity.

4. (Original) The method of claim 1, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

5. (Previously presented) The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment.

6. (Previously presented) The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

7. (Previously presented) The method of claim 1, wherein said preconfigured security update policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

8. (Previously presented) The method of claim 1, wherein said blocking step includes:

instructing a firewall, which is responsive to said preconfigured security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

9. (Previously presented) The method of claim 1, wherein the at least one preapproved host comprises specific security-relevant sites.

10. (Original) The method of claim 9, wherein specific security-relevant sites include antivirus Web sites.

11. (Original) The method of claim 9, wherein specific security-relevant sites include firewall Web sites.

12. (Original) The method of claim 9, wherein specific security-relevant sites include end point security Web sites.

13. (Original) The method of claim 1, wherein other attempted connections to the computer are refused.

14. (Original) The method of claim 1, further comprising:

upon the computer completing updating of security subsystems, removing the restricted zone so that the computer may connect to other machines.

15. (Previously presented) The method of claim 14, wherein the restricted zone is removed by replacing the preconfigured security update policy with an updated security update policy.

16. (Previously presented) The method of claim 1, wherein the preconfigured security update policy is preinstalled on the computer prior to user purchase.

17. (Previously presented) The method of claim 1, wherein the computer includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes the preconfigured security update policy.

18. (Original) The method of claim 1, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

19. (Previously presented) The method of claim 18, further comprising:

providing an option that allows a user to override the preconfigured security update policy.

20. (Previously presented) The method of claim 19, further comprising:

providing a warning to any user that overrides the preconfigured security update policy.

21. (Previously presented) The method of claim 19, further comprising:

displaying a disclaimer to any user that overrides the preconfigured security update policy that indicates that the user assumes responsibility.

22. (Original) The method of claim 9, wherein specific security-relevant sites include operating system-related Web sites.

23. (Original) The method of claim 1, further comprising:

upon a first attempted connection of the computer, downloading an updated list of hosts that the computer may initially connect to.

24. (Original) A computer-readable medium having processor-executable instructions for performing the method of claim 1.

25. (Currently amended) The method of claim 1, further comprising:

~~A downloadable~~ downloading a set of processor-executable instructions for performing the method of claim 1.

26. (Currently amended) A computer system that is preconfigured to control connections upon the initial deployment, the system comprising:

a new computer ~~having~~ that, before deployment, is imaged to include a preconfigured security update policy that establishes a restricted zone of at least one preapproved host that the computer ~~may~~ is restricted to connect to upon the initial deployment of the computer, so that the computer is ~~not allowed to participate with general~~ completely blocked from all other connectivity to the Internet until security-relevant updates have been completed;

a connectivity module for processing user requests for the computer to connect to a particular host; and

a security module, located at the computer, for determining whether the particular host is within the restricted zone of at least one preapproved host based on said preconfigured security update policy, and for blocking any attempt to connect to a host that is not within the restricted zone of at least one preapproved host, until the computer is brought into compliance with the security update policy.

27. (Previously presented) The system of claim 26, further comprising:

a hard disk that receives a hard disk image having said preconfigured security update policy.

28. (Previously presented) The system of claim 26, wherein the computer comprises a portable computer and the initial deployment includes establishing Internet connectivity.

29. (Original) The system of claim 26, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

30. (Previously presented) The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being remotely accessed by another computer upon the initial deployment.

31. (Previously presented) The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

32. (Previously presented) The system of claim 26, wherein said preconfigured security update policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

33. (Previously presented) The system of claim 26, wherein the security module blocks attempts by instructing a firewall, which is responsive to said preconfigured

security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

34. (Previously presented) The system of claim 26, wherein the at least one preapproved host comprises specific security-relevant sites.

35. (Original) The system of claim 34, wherein specific security-relevant sites include antivirus Web sites.

36. (Original) The system of claim 34, wherein specific security-relevant sites include firewall Web sites.

37. (Original) The system of claim 34, wherein specific security-relevant sites include end point security Web sites.

38. (Original) The system of claim 26, wherein other attempted connections to the computer are refused.

39. (Original) The system of claim 26, further comprising:

a module for removing the restricted zone so that the computer may connect to other machines.

40. (Previously presented) The system of claim 39, wherein the restricted zone is removed by replacing the preconfigured security update policy with an updated security update policy.

41. (Previously presented) The system of claim 26, wherein the preconfigured security update policy is preinstalled on the computer prior to user purchase.

42. (Previously presented) The system of claim 26, wherein the computer includes a hard disk having a manufacturer-provided disk image, and wherein the

manufacturer-provided disk image includes said preconfigured security update policy.

43. (Original) The system of claim 26, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

44. (Previously presented) The system of claim 43, wherein the security module includes an option that allows a user to override the preconfigured security update policy.

45. (Previously presented) The system of claim 44, wherein the security module displays a warning to any user that overrides the preconfigured security update policy.

46. (Previously presented) The system of claim 44, wherein the security module displays a disclaimer to any user that overrides the preconfigured security update policy that indicates that the user assumes responsibility.

47. (Original) The system of claim 34, wherein specific security-relevant sites include operating system-related Web sites.

48. (Original) The system of claim 26, wherein the security module downloads an updated list of hosts that the computer may initially connect to.

49. (Currently amended) A method for enforcing pre-access connectivity restrictions on a new machine so as to enforce security updates, the method comprising:

before deployment, incorporating into the new machine an initial security update policy that prevents computer infections occurring before the new computer can obtain security-relevant updates;

detecting attempts to connect the new machine to other devices;

determining at the new machine, based on ~~an~~ said initial security update policy that establishes a restricted zone of acceptable connections, which devices the new machine is permitted to connect to, so that the machine is not allowed to participate with

general connectivity to the Internet until security-relevant updates have been applied to the machine; and

blocking at the new machine any connection that attempts to connect the new machine to a device outside the restricted zone of acceptable connections, so that the machine cannot participate with general connectivity to the Internet until the machine is brought into compliance with the security update policy.

50. (Previously presented) The method of claim 49, further comprising:

prior to the initial deployment of the new machine, imaging a hard disk of the new machine with said initial security update policy.

51. (Previously presented) The method of claim 49, wherein the new machine comprises a portable computer and the initial deployment includes establishing Internet connectivity.

52. (Original) The method of claim 49, wherein said restricted zone comprises a pre-access restricted zone specifically for a new machine.

53. (Previously presented) The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being remotely accessed by another computer upon the initial deployment.

54. (Previously presented) The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being remotely probed for vulnerabilities by other computers.

55. (Previously presented) The method of claim 49, wherein said initial security update policy operates to prevent the new machine from being infected by a malicious program delivered through an open port.

56. (Previously presented) The method of claim 49, wherein said blocking step

includes:

instructing a firewall, which is responsive to said initial security update policy, to block connections to any host that is not within the restricted zone of at least one preapproved host.

57. (Previously presented) The method of claim 56, wherein the at least one preapproved host comprises specific security-relevant sites.

58. (Original) The method of claim 57, wherein specific security-relevant sites include antivirus Web sites.

59. (Original) The method of claim 57, wherein specific security-relevant sites include firewall Web sites.

60. (Original) The method of claim 57, wherein specific security-relevant sites include end point security Web sites.

61. (Original) The method of claim 49, wherein other attempted connections to the new machine are refused.

62. (Original) The method of claim 49, further comprising:

upon the new machine completing updating of security subsystems, removing the restricted zone so that the new machine may connect to other machines.

63. (Previously presented) The method of claim 62, wherein the restricted zone is removed by replacing the initial security update policy with an updated security update policy.

64. (Previously presented) The method of claim 49, wherein the initial security update policy is preinstalled on the new machine prior to user purchase.

65. (Previously presented) The method of claim 49, wherein the new machine includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes said initial security update policy.

66. (Original) The method of claim 49, wherein the new machine is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed.

67. (Previously presented) The method of claim 66, further comprising:

providing an option that allows a user to override the initial security update policy.

68. (Previously presented) The method of claim 67, further comprising:

providing a warning to any user that overrides the initial security update policy.

69. (Previously presented) The method of claim 67, further comprising:

displaying a disclaimer to any user that overrides the initial security update policy that indicates that the user assumes responsibility.

70. (Original) The method of claim 57, wherein specific security-relevant sites include operating system-related Web sites.